611-TD-590-001

EOSDIS Core System Project

M&O Procedures: Section 3—System Administration

Interim Update

July 2001

Raytheon Company
Upper Marlboro, Maryland

Preface

This document is an interim update to the Mission Operations Procedures Manual for the ECS Project, document number 611-CD-600-001. This document has not been submitted to NASA for approval, and should be considered unofficial.

This document has been updated to reflect the removal of DCE mechanisms and HP machines from the baseline and the increased focus on system security.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5301

This page intentionally left blank.

3. System Administration

This section covers the procedures necessary for the System Administrator (SA) and/or Operator (OPR) to manage and operate the system.

Detailed procedures for tasks performed by the System Administrator and/or Operator are provided in the sections that follow. The procedures assume that the administrator and/or operator is authorized and has proper access privileges to perform the tasks (i.e., root) and that the SA and/or OPR has been properly trained in all aspects of the system.

Each procedure outlined will have an **Activity Checklist** table that will provide an overview of the task to be completed. The outline of the **Activity Checklist** is as follows:

Column one - ***Order*** shows the order in which tasks should be accomplished.

Column two - ***Role*** lists the Role/Manager/Operator responsible for performing the task.

Column three - ***Task*** provides a brief explanation of the task.

Column four - ***Section*** provides the Procedure (P) section number or Instruction (I) section number where details for performing the task can be found.

Column five - ***Complete?*** is used as a checklist to keep track of which task steps have been completed.

The following is the **Activity Checklist** table that provides an overview of the overall system administration processes and who performs them

Table 3.1. System Administration - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPR	Secure Shell	(I) 3.1	
2	OPR	System Startup/Shutdown	(I) 3.2	
3	OPR	System Backup and Restore	(I) 3.3	
4	SA	User Administration	(I) 3.4	
5	SA	Security	(I) 3.5	

For procedures outlined in this section, there are corresponding **QUICK STEP** procedures immediately following in this chapter. The **QUICK STEP** procedures are designed for persons who have ***prior training or are experienced system administrators with prior system administration experience.*** The ***QUICK STEP*** procedures should be used by ***experienced persons ONLY***.

3.1 Secure Shell

Secure Shell (SSH) is an applications that greatly improves network security. Secure Shell is the standard for remote logins, solving the problem of hackers stealing passwords. Secure Shell secures connections by encrypting passwords and other data. Once launched, it provides transparent, strong authentication and secure communications over any IP-based connection. The SSH Secure Shell application is virtually invisible during day-to-day use. It provides a provides an extensive library of features for securing and authenticating terminal connections, file transfers or almost any other type of connection might be created over an IP network. Secure Shell is to be used for communication among system platforms and among the DAACs

Table 3.1-1. Secure Shell - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS	Initiating sshsetup	(I) 3.1.1	
2	OPR	Setting up remote access ssh	(I) 3.1.2	
3	OPR	Changing Your Passphrase	(I) 3.1.3	

3.1.1 Setting Up SSH

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing **ssh** commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via SSH. The process is started by running the sshsetup script, which will enable ssh to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

To initialize Secure Shell Access (ssh), execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup**, then press Return/Enter.

- You will see an information statement:

Use a passphrase of at least 10 characters, which should include numbers or special characters and MAY include spaces

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

Initializing random number generator...

Generating p: Please wait while the program completes ...

%

- This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.

3.1.2 Remote SSH Access

If you need to access a host with a different home directory, you will need to run the sshremote script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

To set up remote access shell (ssh), execute the procedure steps that follow:

1 Login into your normal Unix workstation where your home directory resides.

2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote**, then press Return/Enter.

- You will see the following prompt:

You have a local passphrase. Do you want to setup for:

1 VATC

2 EDF

3 MiniDAAC

4 GSFC DAAC

5 GSFC M and O

6 EDC DAAC

7 EDC M and O

8 LaRC DAAC

9 LaRC M and O

10 NSIDC DAAC

11 NSIDC M and O

12 Exit from script

Select:

3 At the "Select" prompt, type in the corresponding number to the desired host, then press Return/Enter.

- You will receive a prompt similar to the following for the VATC:

  Working...

4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** and then press Return/Enter.

- A prompt similar to the following will be displayed:

  Last login: Thu Jul 9 10:41:13 1998 from echuser.east.hit

No mail.

Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996

t1code1{username}1:

5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host

- You will see an information statement:
  Use a passphrase of at least 10 characters, which should include numbers or special characters and MAY include spaces

6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

  Initializing random number generator...

  Generating p: Please wait while the program completes ...

  %

8 At the "t1code1" prompt type **exit**, the press Return/Enter.

- The following information will be displayed:

  Updating locally...

  Updating t1code1u.ecs.nasa.gov

  %

This establishes the ssh key at the remote host and exchanges key information with your local host. Note: The ssh keys at remote sites can be different from the local host ssh key.

3.1.3 Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The ssh keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

To change your Secure Shell Passphrase, execute the procedure steps that follow:

1 Login to your normal Unix workstation where your home directory resides.

- Initiate passphrase change by typing /tools/bin/sshchpass, then press Return/Enter.
- You will see an information statement:

  Use a passphrase of at least 10 characters, which should include numbers or special characters and may include spaces

2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**

3 At the prompt "New passphrase:" **enter your passphrase <enter>**.

4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see an information prompt similar to the following:

  ssh-keygen will now be executed. Please wait for the prompt to Return!

  /home/bpeters/.ssh/authorized_keys permissions have already been set.

  %

3.2 System Startup and Shutdown

The Startup and Shutdown processes begin when it has been determined by the DAAC Operations Supervisor or his designee that it is necessary to stop or start the system. The least impacting method is determined and users are appropriately notified.

When determining the least impacting way to perform the startup or shutdown, the OPR, along with the Operations Supervisor takes into consideration whether only specific server software packages would need to be started/stopped or an entire system startup/shutdown is required.

Once these steps have been taken, the shutdown or startup is performed.

The **Activity Checklist** table that follows provides an overview of the startup and shutdown processes.

Table 3.2-1. Startup/Shutdown - Activity Checklist

Order	Role	Task	Section	Complete?
1	OPS Sup	Determine that Startup/Shutdown is necessary.	(I) 3.2	
2	OPR	Determine the Least Impacting Way to Perform the Startup/Shutdown.	(I) 3.2	
3	OPR	Notify Those Effected by the Startup/Shutdown.	(I) 3.2	
4	OPR	Perform the Startup/Shutdown	(P) 3.2	

3.2.1 Startup

Startup means that power to the system is restored and the system is being taken to a fully useable and operational state.

3.2.1.1 Cold - By Subsystem

A cold startup means that power to the system has been previously powered off and the system(s) is being restarted from this cold state. The System Startup process begins after a previously completed shutdown, either scheduled or emergency. The System Startup is done in sequential order by subsystem. The SA predetermines this startup sequence.

This procedure assumes that the OPR has been properly trained to startup all aspects of the system and that the system is currently powered off (due to a normal or emergency shutdown).

The procedure assumes that the Startup has been scheduled well in advance, all planning involved has been concluded well in advance and all other Distributed Active Archive Centers (DAACs) have been notified of the system returning to an on-line state.

This section explains how to perform a cold system startup by subsystem. The sequence of the execution of the steps below is very important. To begin a cold system startup, execute the procedure steps that follow:

1 The sequence of booting the machines is important:

- Remember to power on peripherals before powering on each CPU.
- Monitor each system Boot Up activity on that system's monitor.
- The DNS and NIS servers must be booted first.
- Once each system has booted without error, proceed to the next machine**.** Boot the machines according to Table 3.2-2. This table presents the cold system startup machine boot sequence. The machine names are to be added once identified by each DAAC SA for a specific baseline.

2 Continue booting the remaining machines.

Table 3.2-2. Cold System Startup - Machine Boot Sequence

Step	What to Enter or Select	Action to Take (Server)	Machine Name
1	(No entry)	NIS Master	**x0css02**
2	(No entry)	DNS Master	**x0css02**
3	(No entry)	ClearCase Server(s)	**x0mss0x**
	(No entry)	Interface Server(s)	**x0ins0x**
4	(No entry)	MSS: Tivoli Server	**x0mshxx**
5	(No entry)	DSS	**x0acs0x**
6	(No entry)	Ingest	**x0icg0x**
7	(No entry)	PDPS	**x0pls0x**
8	(No entry)	Others	

3.2.1.2 Warm - By Subsystem Startup

A warm startup means the system has been previously powered on, but the system(s) is not fully operational, either the system has had some service performed (i.e. single user mode) or is being rebooted to correct some minor malfunction. The System Startup is done in sequential order by subsystem. This startup sequence is predetermined by the software dependencies.

The order of the re-boot is contingent on software dependencies per site.

If the NIS servers service has been interrupted, the users will automatically be transferred to a backup server. Once the faulty server(s) has been repaired, re-establish connection with the primary NIS server by rebooting the Backup Server; the users would then be transferred back to the primary NIS server.

Table 3.2-3 presents the **QUICK STEP** procedure required to perform a warm system startup.

Table 3.2-3. Warm System Startup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	determine software dependencies
2	(No entry)	reboot independent server(s)
3	(No entry)	reboot dependent server(s)

Note: In addition to warm system startup/reboot sequences, ECS servers that use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted, once the Sybase SQL server has come back on-line.

3.2.1.3 Additional tasking - Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Program Generated Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are ${PGSHOME}/database/common/TD/leapsec.dat and ${PGSHOME}/database/common/CSC/utcpole.dat. The update of these files is accomplished by executing leapsec_update.sh and utcpole_update.sh in the /tools/admin/exec directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting .

3.2.2 Shutdown

Shutdown means that the system is being removed from a fully useable and operational state and possibly, power to the system will be terminated. The types of shutdown would vary depending upon circumstances (i.e. shutdown to single user mode; shutdown to power off; etc.)

3.2.2.1 Normal - By Subsystem

The Normal System Shutdown process is performed at the discretion of the SA usually for a scheduled repair. The system shutdown is **normally performed in reverse order of the system startup.**

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the OPR/SA has been properly trained to shutdown all aspects of the system.

This section explains how to perform a normal system shutdown by subsystem**.**

3.2.2.1.1 Shutdown a Machine

The OPR must be logged in as root to perform a shutdown. To begin a normal system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **wall** and press **Return**. Use **wall -a** on Sun machines to cross NFS mounts.

4 Type **This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.** then press **Return.** Press **Control** and **D** keys **simultaneously**. Include your name and closest telephone number.

5 Wait at least five minutes.

6 Type **shutdown -g600 -i0 -y** UNIX prompt and press **Return**. (600 = Number of Seconds)

7 When the system is at the prompt, it is safe to ***Power off*** all peripherals first and then the CPU.

The servers should be shutdown in the reverse order of the startup:

1 Determine which machines are dependent on a server first:
- Once each system has stopped without error, power off peripherals
- Proceed to the following machine

- Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine for each machine

2 The **NIS server** must be the **last system** to be shutdown.

Table 3.2-4 presents the **QUICK STEP** procedure required to perform a normal system shutdown.

Table 3.2-4. Normal System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**Determine subsystems and server dependencies**
2	(No entry)	**Login to the server as root**
3	**wall**	**Press Return**
4	**This machine is being shutdown for *reason*. The anticipated length of down time is *xxx*. Please save your work and log off now. The machine will be coming down in *xxx* minutes. We are sorry for the inconvenience.**	**Press Control and D keys simultaneously**
5	(No entry)	**Wait at least five minutes**
6	**shutdown -g600 -i0 -y** **- OR -** **shutdown now -i0 -y**	**Press Return**
7	(No entry)	**Power off all peripherals and the CPU.**
8	(No entry)	**Repeat steps 2 through 7 above for all servers Table 3.2.2**

3.2.2.2 Emergency - By Subsystem

The Emergency System Shutdown process begins after the System Administrator determines that the system may fail during emergency situations (e.g., storms, power outages). The Emergency System Shutdown is done in sequential order by subsystem. This shutdown sequence is pre-determined by the SA.

The NIS servers must be the last system to shutdown.

Detailed procedures for tasks performed by the OPR/SA are provided in the sections that follow.

This section explains how to perform an emergency system shutdown by subsystem. The OPR must be logged in as root to perform a shutdown. To begin an emergency system shutdown, execute the procedure steps that follow:

1 Login to the server as root.

2 Enter root password.

3 Type **sync** at the UNIX prompt and hit **Return**.

Sync executes the sync system primitive. If the system is to be stopped, sync must be called to insure file system integrity. It will flush all previously unwritten system buffers out to disk, thus assuring that all file modifications up to that point will be saved.

4 Type **sync** again at the UNIX prompt and hit **Return**.

5 Type **halt** at the UNIX prompt and hit **Return**.

6 Once the halt has completed, turn the power switch on all the peripherals and the CPU off.

The servers should be shutdown in the following order:

1 Shutdown all client workstations.

2 ***Follow steps 1-7 for Task: 3.2.2.1.1 Shutdown Machine*** *for* ***each*** *machine*

3 The **NIS servers** must be the **last systems** to shutdown.

In case of ***EXTREME emergency*** where time does not allow you to execute the above procedures, execute the following procedure steps for ***Sun machines ONLY.***

1 Login to the server as root.

2 Enter root password.

3 Hit the L1 or Stop key and the a key simultaneously.

4 Once returned to an **ok** or > prompt, turn the power switches on the CPU and all peripherals to off.

NOTE: The use of L1a does not ensure file system integrity. There is a very high risk of losing data when using this process.

Table 3.2-5 presents **QUICK STEP** procedures required for Emergency System Shutdown.

Table 3.2-5. Emergency System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine subsystems and server dependencies**
2	(No entry)	**Login to server as root**
3	(No entry)	**Type sync at prompt and press enter**
4	(No entry)	**Type sync at prompt and press enter**
5	(No entry)	**Type halt at prompt and press enter**
6	(No entry)	**Turn power switches on CPU and all peripherals to off.**
7	(No entry)	**Repeat steps 2 through 5 above for all servers**

3.2.2.3 Server - By Server Software

The System Shutdown by Server Software process is performed by the OPR. The system shutdown is normally performed in reverse order of the system startup.

The procedures assume that the Shutdown has been scheduled well in advance, all planning involved has been concluded well in advance and the SA has been properly trained to shutdown all aspects of the system.

Table 3.2-6 presents the **QUICK STEP** procedure required to perform a normal system shutdown.

Table 3.2-6. Server System Shutdown - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	(No entry)	**determine software dependencies**
2	(No entry)	**shutdown dependent server(s)**
3	(No entry)	**shutdown independent server(s)**

3.3 System Backup and Restore

System Backup and Restore is the process of copying, either the entire or partial system, the information from the machine for safe keeping for a specific time period. Restore is the process of returning the data to the machine to allow operation to continue from a specific point in time. The OPR must be in the admin list to use Networker. This is not root privilege.

3.3.1 Incremental Backup

Non-scheduled incremental backups can be requested at any time by submitting a request for ***Incremental Backup*** to the **OPS supervisor**. The supervisor schedules the request with the OPR who performs the incremental backup. Afterwards, the OPR notifies the requester and supervisor that the incremental backup is complete.

The **Activity Checklist** table that follows provides an overview of the incremental backup processes.

Table 3.3-1. Incremental Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for **Incremental** Backup to OPS Supervisor.	(I) 3.3.1	
2	OPS Super	Schedule Incremental Backup with OPR	(I) 3.3.1	
3	OPR	Perform Incremental Backup.	(P) 3.3.1	
4	OPR	Notify Requester and OPS Super when Incremental Backup is Complete.	(I) 3.3.1	

Detailed procedures for tasks performed by the OPR are provided in the sections that follow.

The procedures assume that the requester's request for an incremental backup has already been approved by DAAC Management. Incremental backups can be requested at any time by submitting a request for ***Full Backup*** to the **OPS supervisor**. In order to perform the procedure, the OPR must have obtained the following information from the requester:

a. **Name of machine to be backed up**

b. **Files/directories to be backed up (optional)**

To perform an incremental backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.3.5.1 Labeling Tapes and then return to this procedure.

1 Log into the **machine to be backed up** by typing: **ssh** ***BackedUpSystemName***, then press **Return**.

2 At the Passphrase promt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get the Password prompt.

3 Enter ***YourPassword***, then press **Return.**
- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press **Return**.
- A password prompt is displayed.

5 Enter the ***RootPassword***, then press **Return**.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the NetWorker Administrative program by entering: **nwadmin &**, then press **Return**.
- A window opens for the NetWorker Administrative program.
- You are now able to perform an incremental backup.

7 Click Clients.
- Click Client Setup
- Click Host Being Backed Up
- Highlight the group to be Backed Up

8 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

9 Look at the button for today. If there is an **i** next to the date on this button, go to step 12.

- The **i** stands for incremental.
- The **f** stands for full.

Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.

10 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.

11 Click the **Apply** button.

12 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

13 Click the **Group Control** button.

- The **Group Control** window opens.

14 Click the **Start** button.

- A **Notice** window opens.

15 Click the **OK** button.

- The **Notice** window closes.
- The regularly scheduled backup will still run (even though we are now doing a backup).

16 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.

- Status updates appear in the **nwadmin** window.
- When the backup is complete, a **Finished** message will appear.

17 If the button for today in step 9 had an **i** on it, go to step 21.

18 Go to the **Customize** menu, select **Schedules**.

- The **Schedules** window opens.

19 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.

20 Click the **Apply** button.

21 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.

22 Select **Exit** from the **File** menu to quit the NetWorker Administrative program.

- The **nwadmin** window closes.

23 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.

- **Root** is logged out.

24 Type **exit** again, then press **Return**.

- You are logged out and disconnected from the **machine to be backed up**.

Table 3.3-2 presents the **QUICK STEP** procedure required to perform an incremental backup.

Table 3.3-2. Perform Incremental Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** *BackedUpSystemName*	**press Return**
2	*YourPassphrase* **or-** (No entry)	**press Return -or-** (No action)
3	*YourPassword*	**press Return**
4	**su**	**press Return**
5	*RootPassword*	**press Return**
6	**nwadmin**	**press Return**
7	Click Client Click **Client Setup** Click Host Being Backed Up **-** Highlight the Group to be Backed Up	
8	**Customize → Schedules**	**if i on today's button then go to step 9. Otherwise, click and hold today's button.**
9	**Overrides → Incremental**	**click Apply button**
10	(No entry)	**close Schedules window**
11	(No entry)	**click Group Control button**
12	(No entry)	**click Start button**
12	(No entry)	**click OK button**
14	(No entry)	**close Group Control window**
15	(No entry)	**if there was an i on today's button in step 8, go to step 17.**
16	**Customize → Schedules**	**click and hold today's button**
17	**Overrides → Full**	**click Apply button**
18	(No entry)	**close Schedules window**
19	**File → Exit**	(No action)
20	**exit**	**press Return**
21	**exit**	**press Return**

3.3.2 Full Backup

Non-scheduled full backups can be requested at any time by submitting a for ***Full Backup*** to the OPS supervisor. The supervisor schedules the request with the OPR who performs the full backup. Afterwards, the OPR notifies the requester and supervisor that the full backup is complete.

The **Activity Checklist** table that follows provides an overview of the full backup processes.

Table 3.3-3. Full Backup - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for **Full** Backup to OPS Supervisor.	(I) 3.3.2	
2	OPS Super	Schedule Full Backup with **OPR**	(I) 3.3.2	
3	OPR	Perform Full Backup.	(P) 3.3.2	
4	OPR	Notify Requester and OPS Super when Full Backup is Complete.	(I) 3.3.2	

Detailed procedures for tasks performed by the OPR are provided in the sections that follow.

The procedures assume that the requester's application for a full backup has already been approved by DAAC Management. In order to perform the procedure, the OPR must have obtained the following information from the requester:

a. **Name of machine to be backed up**

b. **Files/directories to be backed up** (optional)

To perform a full backup for the requester, execute the procedure steps that follow:

Note 1: If you run out of tapes at any time during this procedure, execute procedure 3.3.5.1 Labeling Tapes and then return to this procedure.

1 Log into the **machine to be backed up** by typing: **ssh** ***BackedUpSystemName***, then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get to Password prompt.

3 Enter ***YourPassword***, then press **Return.**
- Remember that ***YourPassword*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Log in as root by typing: **su**, then press **Return**.
- A password prompt is displayed.

5 Enter the ***RootPassword***, then press **Return**.
- Remember that the ***RootPassword*** is case sensitive.
- You are authenticated as root and returned to the UNIX prompt.

6 Execute the NetWorker Backup program by entering: **nwbackup &**, then press **Return**.
- A **NetWorker Backup** window opens.
- You are now able to perform a full backup.

7 Click Clients.
- Click Client Setup
- Click Host Being Backed Up
- Highlight the group to be Backed Up

8 If no list of **files/directories to be backed up** was provided, i.e. the whole machine is to be backed up, then type **/** in the **Selection** field and click the **Mark** button.
- / is designated for backup and has a check next to it.

9 If names of **files/directories to be backed up** were provided then select the **files/directories to be backed up** in the directory display and click the **Mark** button.
- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.
- To move up a directory level, type the path in the **Selection** field.
- Clicking the **Mark** button designates the file for backup and puts a check next to it.

10 Click the **Start** button.
- A **Backup Options** window opens.

11 Click the **OK** button.
- The **Backup Options** window closes.
- The **Backup Status** window opens providing updates on the backup's progress.

12 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.
- The **Backup Status** window closes.
- The backup is complete.

13 Select **Exit** from the **File** menu to quit the NetWorker Backup program.
- The **NetWorker Backup** window closes.

14 At the UNIX prompt for the **machine to be backed up**, type **exit**, then press **Return**.
- **Root** is logged out.

15 Type **exit** again, then press **Return**.
- You are logged out and disconnected from the **machine to be backed up**.

To perform a full backup, execute the steps provided in the following table.

Table 3.3-4 presents the **QUICK STEP** procedure required to perform a full backup.

Table 3.3-4. Perform Full Backup - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** *BackedUpSystemName*	**Press Return**
2	*YourPassphrase* **or-** (No entry)	**Press Return -or-** (No action)
3	*YourPassword*	**Press Return**
4	**su**	**Press Return**
5	*RootPassword*	**Press Return**
6	**nwbackup &**	**Press Return**
7	Click Client Click **Client Setup** Click Host Being Backed Up - Highlight the Group to be Backed Up	
8	**to back up whole machine, place / in selection field**	**Click Mark button**
9	**to back up certain files/directories, indicate the files/directories**	**Click Mark button**
10	(No entry)	**Click Start button**
11	(No entry)	**Click OK button**
12	(No entry)	**Click Cancel button**
13	**File → Exit**	(No action)
14	**exit**	**Press Return**
15	**exit**	**Press Return**

3.3.3 File Restore

From time to time, individual files or groups of files (but not all files) will have to be restored from an Incremental or Full backup tape(s) due to Operator error or system failure. This can be accomplished using the following file restoration procedure.

The File Restore process begins when the requester submits a request to the Operator. The Operator restores the file(s) and notifies the requester when complete.

The Activity Checklist table that follows provides an overview of the file restore process.

Table 3.3-5. File Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request for File Restore to Operator	(I) 3.3.3	
2	Operator	Restore file(s).	(P) 3.3.3	
3	Operator	Inform Requester of completion.	(I) 3.3.3	
4	Operator	Complete System Restore/Partition Restore	(P) 3.3.3	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow. The procedures assume that the requester's application for a file restore has already been approved by the Ops Supervisor. In order to perform the procedure, the Operator must have obtained the following information from the requester:

a. **Name of machine to be restored**

b. **Name of file(s) to be restored**

c. **Date from which to restore**

d. **User ID of the owner of the file(s) to be restored**

e. **Choice of action to take when conflicts occur. Choices are:**

- **Rename current file**
- **Keep current file**
- **Write over current file with recovered file**

Table 3.3-6 represents the steps required to restore a file in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the detailed procedures presented below.

To restore a file for the requester, execute the procedure steps that follow:

1 Log into the **machine to be restored** by typing: **ssh**, then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**
- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt..

NOTE: Before executing the NetWorker Recovery ensure, that you are in the /data1/COTS/networker directory.

4 Execute the **NetWorker Recovery** program by entering: **nwrecover &**, then press **Return**.
- A window opens for the Networker Recovery program.
- You are now able to perform the file restoration.

5 Select **file(s) to be restored** and click the **Mark** button.
- Drag scroll bar with mouse to scroll the list up and down.
- Double click on directory name to list its contents.

- Clicking the Mark button designates the file for restore and places a check in the box adjacent to the file or directory name.

6 Go to the **Change** menu, select **Browse Time**.
- The Change Browse Time window opens.

7 Select the **date from which to restore**.
- **NetWorker** will automatically go to that day's or a previous day's backup which contains the file.

8 Click the **Start** button.
- The Conflict Resolution window opens.

9 Answer **Do you want to be consulted for conflicts** by clicking the **yes** button, then click the **OK** button.
- If prompted with a conflict, choices of action will be: **rename current file**, **keep current file**, or **write over current file with recovered file**. Select the requesters **choice of action to take when conflicts occur**.
- The Recover Status window opens providing information about the file restore.
- If all the required tapes are not in the drive, a notice will appear. Click the **OK** button in the notice window.
- If prompted for tapes, click cancel in the **Recover Status** window and execute procedure 3.2.5-2 Index Tapes.

10 When a recovery complete message appears, click the **Cancel** button.

11 Go to the **File** menu, select **Exit**.
- The **NetWorker Recovery** program quits.

12 Type **exit**, then press **Return**.
- The **owner of the file(s) to be restored** is logged out.

13 Type **exit** one last time, then press **Return**.
- You are logged out and disconnected from the **machine to be restored.**

To restore a file, execute the steps provided in the following table.

Table 3.3-6. Restore a File - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh** to the *Machine to be Restored*	**press Return**
2	*Your Passphrase* **-or-** (No entry)	**press Return -or-** (No action)
3	*Your Password*	**press Return**
4	**nwrecover &**	**press Return**
5	**file(s) to be restored**	**click the Mark button**
6	**Change → Browse Time**	(No action)
7	**date from which to restore**	**click the Start button**
8	**yes**	**click OK button**
9	(No entry)	**choose what action to take when notified of conflicts**
10	(No entry)	**click Cancel button**
11	**File → Exit**	(No action)
12	**exit**	**press Return**
13	**exit**	**press Return**
14	**exit**	**press Return**

3.3.4 Complete System Restore

The Complete System Restore process begins when the requester has determined that a complete system restore is the only way to resolve the problem and has approval from the Operations Supervisor. Once notified of the request, the Operator performs restores of all partitions on the system. Afterwards, the Operator documents and logs all actions in the operator's log book and notifies the requester and Ops Supervisor that the system restore is complete.

The Activity Checklist table that follows provides an overview of the complete system restore process.

Table 3.3-7. Complete System Restore - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Trouble Shoot and Determine that a Complete System Restore is necessary.	(I) 3.3.4	
2	Operator	Restore all Partitions on the System	(P) 3.3.4	
3	Operator	Document and Log in operator's log book, and Inform Requester and Ops Supervisor of completion.	(I) 3.3.4	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow. The procedures assume that the requester's application for a complete system restore has already

been approved by Ops Supervisor. In order to perform the procedures, the Operator must have obtained the following information about the requester:

a. **Name of system to be restored**

b. **Date from which to restore**

A complete system restore involves restoring all partitions on that system.

Table 3.2-8 presents the steps required to restore a partition in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed these tasks recently, you should use the detailed procedures presented below.

To restore a partition for the requester, execute the procedures steps that follow:

1 Log into the backup server by typing: **ssh *machine to be restored,*** then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**
- Remember that ***Your Password*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Execute the **NetWorker Administrative** program by entering: **nwadmin &,** then press **Return**.
- A window opens for the NetWorker Administrative program.
- You are now able to perform restores of partitions.

5 Go to the **Save Set** menu, select **Recover Set.**
- The **Save Set Recover** window opens.

6 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.
- The **Save Set** listing updates. This is a listing of partitions on the **System**.
- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.

7 Select the **Save Set**/partition from the listing.
- The **Instance** listing updates.

8 Select the appropriate **Instance**.
- An Instance is a particular Networker client backup. A listing of Instances is a report detailed with the Networker client backups that have occurred.

- Select an Instance based upon the Date from which to restore(referred to as Date in the rest of this procedure) and an appropriate level:

*__NOTE__ 1: To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backups occur at 02:00 each morning, then a system corrupted at noon on June 6th would require a restoration of the June 6th backup. If the Backups are full or incremental, perform the following actions: Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.

If the backups are of different numerical levels, follow these steps:

1) Select the most recent level **0/full backup** prior to or on the **Date** and perform a restore of the partition.
2) If a level **0/full backup** did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level **0** and prior to or on the **Date**.
3) Perform a restore of the partition.
4) Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.

- You can double click an **Instance** to see which tape is required.

9 Click the **Recover** button.
- The Save Set Recover Status window opens.
- Clicking the Volumes button will show which tapes are required.

10 Click the **Options** button.
- The **Save Set Recover** Options window opens.

11 Set **Duplicate file resolution** to **Overwrite existing file** by clicking its radio button.

12 Make sure that the **Always prompt** checkbox is not checked.

13 Click the **OK** button.
- The Save Set Recover Options window closes.

14 Click the **Start** button in the **Save Set Recover Status** window.
- Status messages appear in the Status box.
- If prompted for tapes, click the Cancel button in the **Save Set Recover Status** window and follow steps **1-18** of procedure **3.3.5.2** Index tapes(or steps 1-19 of procedures **3.3.5.2** Index Tapes Quick Steps)
- A **recovery complete** message appears when recovery is complete.

15 Click the **Cancel** button after the **recovery complete** message appears.

- The Save Set Recover Status window closes.

16 If additional partition restores are required, go to step **8**. Otherwise, select **Exit** from the **File** menu to quit the NetWorker Administrative program.

17 At the UNIX prompt for the backup server, type **exit**, then press **Return**.

18 Type **exit** again, then press **Return**.

To restore a partition, execute the steps provided in the following table.

Table 3.2-8. Restore a Partition - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh *to the host which requires partition restoration***	**press Return**
2	*Your Passphrase*	**press Return – or -**
3	*Your Password*	**press Return**
4	**nwadmin &**	**press Return**
5	**Save Set → Recover Set**	(no action)
6	**Client/System**	(no action)
7	**Save Set/partition**	(no action)
8	**Instance**	**click Recover button**
9	(No entry)	**click Options button**
10	**Overwrite existing file**	**deselect Always prompt**
11	(No entry)	**click OK button**
12	(No entry)	**click Start button**
13	(No entry)	**click Cancel button**
14	(No entry)	**go to step 7 -or-** **select File → Exit**
15	**exit**	**press Return**
16	**exit**	**press Return**

3.3.5 Tape Handling

The following procedures demonstrate how to label tapes, index tapes, and clean tape drives. Each of these procedures contains detailed steps that explain how to complete the procedure properly. Each tape handling procedure is significant in maintaining a working backup system. DAAC scheduled backups depend on proper maintenance of tape media and tape drives. Listed are complete explanations of the procedures and their relevance to the Computer Operator position.

The Activity Checklist table that follows provides an overview of the tape handling process.

Table 3.3-9. Tape Handling - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Labeling Tapes	(I) 3.3.5.1	
2	Operator	Indexing Tapes	(P) 3.3.5.2	
3	Operator	Tape Drive Cleaning	(P) 3.3.5.3	

3.3.5.1 Labeling Tapes

The Tape Labeling process begins when the Operator is performing procedures 3.3.1 Incremental Backup or 3.3.2 Full Backup (or their associated Quick Steps) and runs out of tapes. The tape(s) must be installed in the jukebox and labeled. NetWorker uses tape labels for identification. The label that NetWorker creates is on the tape media itself, rather than a sticker on the outside of the tape cassette. An index is kept by NetWorker associating tape labels with particular backups/data. When you select files to be recovered using the NetWorker Recovery window or view saved sets on a backup volume using the Volume Management window in NetWorker, you are viewing this index. After labeling the required tape(s), the Operator resumes procedure 3.2.1 or 3.2.2.

Table 3.3-10. Labeling Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Install Required Tape(s) in Jukebox	(P) 3.3.5.1.1	
2	Operator	Label 8mm Tapes	(P) 3.3.5.1.2	
3	Operator	Label DLT Tapes	(P) 3.4.5.1.3	

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

3.3.5.1.1 Install Required Tape(s) in Jukebox

The procedures assume that the Operator was previously executing procedure 3.3.1 or 3.3.2. In order to perform the procedures, the Operator must have obtained the following:

a. **Blank tape(s)**

All tapes are stored in the storage cabinet located in the control room. There are five tapes in each box, and every box of tapes has a unique number. To begin finding tapes for recycling to be labeled and installed in the Juke box, the lowest numbers of a tape or a box of tapes should be used. Do not recycle any tape or box of tapes that the numbers are higher or current.

3.3.5.1.2 8mm or D3 Tapes Labeling Process

Table 3.3.5-2 presents the steps required to label tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To label tapes, execute the procedure steps that follow:

1 Log into the **backup server** by typing: **ssh *appropriate server (i.e. gsfcsrvr7)*,** then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return**.
- Remember that ***Your Password*** is case sensitive.
- You are authenticated as yourself and returned to the UNIX prompt.

4 Execute the **NetWorker Administrative** program windows by entering: **nwadmin &**, then press **Return**.
- The **NetWorker Administrative** program windows displayed
- Remove all non-blank tapes from the cartridge.
- ***Dismount the drive(s) that will be used for tapes Labeling***

5 Insert the blank tape(s) in the jukebox's cartridge, then install the cartridge in the jukebox.

6 Click the **Label** button from the menu bar.
- The **Jukebox Labeling** window opens.

7 Enter **tape one** in the non-removable **Slot field**.
- **Slot 1** is at the top of the cartridge, and it is a non-removable slot. **Slot 2** through **Slot 11** are removable slots. **Slot 11** contains a cleaning tape. Do not enter any tape in Slot 11 for labeling. The default setting is **1** through **10** for only the tapes that will be labeled and used for backup.
- It is ok to have empty slots.

8 Click the **OK** button.
- A status message appears and updates.
- Labeling a full cartridge of tapes takes about one and half hours. Nine Minutes per tape.

9 When the status in the **Jukebox Labeling** window reads finished, click the **Cancel** button.

- The **Jukebox Labeling** window closes.

10 Go to the **File** menu, select **Exit**.

11 Put a sticker on the outside of each tape cassette.

- This is done in order for you to identify each tape.

11 Resume procedure 3.3.1 or 3.3.2.

To label tapes, execute the steps provided in the following table.

3.3.5.1.3 Label DLT Tapes

The dlt tape labeling process is the same as the 8mm tape labeling scenarios, except for some few things that are additionally different. Steps to follow in labeling the dlt tapes as follow: Repeat Table **3.3.5.1** step 1 through step 9. Change default to **SPRDLT,** then click OK button. The system will display the beginning number of the tape label. Once again repeat step 11 through step 17 of Table **3.3.5.1**, tape labeling process to end the task.

Table 3.3-11. Label Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh***to* ***appropriate server (i.e. gsfcsrvr7)***	**press Return**
2	*Your*Passphrase	**press Return – or -**
3	*Your Password*	**press Return**
4	No Entry	**press Return**
5	**nwadmin &**	**press Return**
6	(No entry)	**put blank tape(s) in cartridge and install cartridge in jukebox**
7	(No entry)	**click Label button**
8	**2**	(No action)
9	**11**	**click OK button**
10	(No entry)	**click Cancel button**
11	**File → Exit**	(No action)
12	**exit**	**press Return**
13	**exit**	**press Return**
14	(No entry)	**put a sticker on the outside of each tape**
15	(No entry)	**resume previous procedure**

3.3.5.2 Indexing Tapes

The Indexing Tapes process begins when the Operator has finished performing procedures 3.3.5.1, (**Tape Labeling**). If the tape(s) is/are not ***indexed/inventoried,*** Networker will not be aware of it/them. After indexing the required tape(s), the Operator resumes procedure 3.3.1 or 3.3.2.

The Activity Checklist table that follows provides an overview of the indexing tapes process.

Table 3.3-12. Indexing Tapes - Activity Checklist

Order	Role	Task	Section	Complete?
1	Operator	Pull Required Tape(s) from Tape Storage.	(I) 3.3.5.2.1	
2	Operator	Index Tapes	(P) 3.3.5.2.2	

3.3.5.2.1 Pull Required Tape(s) from Tape Storage

In order to perform the procedure, the Operator must have obtained the following:

a. **The required tape(s)**

3.3.5-2 Index Tapes

Detailed procedures for tasks performed by the Operator are provided in the sections that follow.

The procedures assume that the Operator has previously executed procedure 3.3.5.1, **Tape Labeling**.

Table **3.3-5-2** presents the steps required to index tapes in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To index tapes, execute the procedure steps that follow:

NOTE: You may proceed to step **8** if you are still logged into the backupserver.

1 Log into the **backup server** by typing: **ssh** ***appropriate server (i.e. gsfcsrvr7),*** then press **Return**.

2 At the Passphrase prompt: enter ***YourPassphrase***, then press **Return**.
- Or press **Return** twice to get to the Password prompt.

3 Enter ***Your Password***, then press **Return.**
- Remember that your password is case sensitive.
- You are authenticated as yourself and returned to the Unix prompt.

4 Execute the **Networker Administrative** program by entering: **nwadmin &,** then press **Return**.

- The Networker Administrative program windows is displayed.
- You are now able to index tapes.
- Click the Mount button to show what tapes **Networker** is currently aware of. The **Jukebox Mounting** windows opens. Once you have finished with this window, click the **Cancel** button.

5 Put the **required tape(s)** in the jukebox's cartridge, install the cartridge in the jukebox.

- For instructions, refer to the jukebox's documentation.

6 Go to the **Media** menu, select **Inventory**.

- The **Jukebox Inventory** window opens.

7 Enter **1** in the **First Slot** field, enter **10** in the **Last Slot** field.

- Slot 1 is the non-removable slot within the jukebox.
- Slot 2 is the first top of the removable cartridge and 11 at the bottom, and it contains a cleaning tape. A default setting 1 through 10.
- It is OK to have empty slots or slots with tapes which have already been indexed.

8 Click the **OK** button.

- A checking volume message appears and updates.
- Performing an inventory on a full cartridge takes about forty minutes.

9 When the status in the **Jukebox Inventory** window says finished, click the **Cancel** button.

- The **Jukebox Inventory** window closes.

10 Click the **Mount** button to verify that the indexing worked.

- The Jukebox Mounting window opens.
- The required tape(s) should be shown. If not, repeat from step 8.

11 Click the **Cancel** button.

- The **Jukebox Mounting** window closes.

12 Go to the **File** menu, select **Exit**.

13 At the UNIX prompt for the ***backup server***, type **exit**, then press **Return**.

14 Type **exit** again, then press **Return**.

15 Resume procedure 3.3.3 at step 12, procedure 3.3.3 at quick-step 11 - action part, procedure 3.3.4 at step 12, or procedure 3.3.4 at quick-step 11 - action part.

To index tapes, execute the steps provided in the table.

Table 3.3-13. Index Tapes - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**ssh *appropriate server (i.e. gsfcsrvr7)***	**press Return**
2	*Your Passphrase*	**press Return - or -**
3	*Your Password*	**press Return**
4	**nwadmin**	**press Return**
5	(No entry)	**put required tape(s) in cartridge and install cartridge in jukebox**
6	**Media → Inventory**	(No action)
7	**2**	(No action)
8	**11**	**click OK button**
9	(No entry)	**click Cancel button**
10	(No entry)	**click Mount button**
11	(No entry)	**verify indexing**
12	(No entry)	**click Cancel button**
13	**File → Exit**	(No action)
14	**exit**	**press Return**
15	**exit**	**press Return**
16	(No entry)	**resume previous procedure**

3.3.5.3 Tape Cleaning Process

The system will at times prompt for drive(s) cleaning. This happens usually during non-processing periods. However, the drive(s) may send a request for cleaning during the course of the tape backup process period,. Manual cleaning should be performed each time tapes are installed in the Juke Box. Maintaining clean drives can help prevent backup interruption, which may occur due to unclean tape drive heads. If the system is prompted for drive(s) cleaning: Follow the details steps below:

1 Log into the Backup Server by typing: **ssh *appropriate server (i.e. gsfcsrvr7)***, then press **Return.**

- The system prompts for your Passphrase

- Type yourPassphrase, then press **Return.**
  - Or press **Return** twice to get to the Password prompt.
- Type your **password,** then press **Return.** Remember, your password is case sensitive.
- Execute Net Worker by typing: **nwadmin &**, then press Return.
  - A NetWorker administrative program windows displayed.
- Highlight the desirable drive(s) that the system has prompted for cleaning.
- Click dismount from the menu bar and wait a few minutes for the drive to be dismounted completely. Repeat step 6 on the second drive until the both are dismounted.

To open the Exabyte door turn the key in the door counter clockwise. The last tape at the bottom of the cartridge is the cleaning tape. Remove it from the slot field and insert it gently into each

drive below. Wait until the tape has been ejected and the flashing lights on the drive are off before removing the tape from the drive. Insure that the cleaning tape is still usable before each use. Cleaning tapes will expire after several uses. After each use mark the appropriate box on the surface of the tape to maintain a list of usage. Insert the cleaning tape back into the last slot and lock the Exabyte door.

3.4 User Administration

3.4.1 Screening Personnel

3.4.1.1 Screening Criteria

Some positions require special access privileges in order to do the assigned job or duties. These are called public trust positions because they can affect the integrity, efficiency, or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior to being granted access, is required. This screening, National Agency Check (NAC), is required to ensure that granting any special access privileges to someone would not cause undue risk to the system for which that employee has these privileges. Line Management is responsible for requesting suitability screening for the employees in their respective organizations.

OMB Circular A-130, Appendix III and NPG 2810.1 requires the following employees to undergo personnel screening:

- All employees who require privileged access or limited privileged access to a Federal computer system or network.
- Privileged access – Can bypass, modify, or disable the technical or operational system security controls.
- Limited privileged access – Can bypass, modify or disable security controls for part of a system or application but not the entire system or application.

Internet Protocol Operational Network (IOnet) Access Protection Policy and Requirements 290-004 requires the following employees to undergo suitability screening:

- All employees who require privileged access, limited privileged access, or access to the Closed Segment of the Internet Protocol Operational Network (IOnet) (formerly NASCOM).
- All employees having access to IOnet network control devices.

NPG 1620.1 requires that all employees granted unescorted access to a NASA Resource Protection (NRP) facility or area and/or a NASA-designated Limited Area undergo screening.

3.4.1.2 Screening Procedures

The line manager will submit NASA Form 531 containing the following information for each employee needing suitability screening.

- Full name (first, middle initial and last)
- Goddard badge number if badged employee
- Reason for requesting screening
- Type and date of any previous security investigation or clearance if known
- Phone number and email address

The request should be sent to the EDF Security Administrator. The GSFC Security Office (GSO) will search the personnel security database to determine if a current NAC has been performed. If not the employee will be contacted to obtain additional information. The GSO will report a favorable or unfavorable result back to the EDF Security Administrator upon completion of the suitability screening.

3.4.2 Adding a User

The Adding a User process begins when the requester fills out a "User Registration Request Form" (located in Appendix A), and submits it to the site supervisor. The "User Registration Request Form" includes information regarding the user (User's Name, Group, Organization, etc.), as well as the user's explanation of why an account on the system is needed. The requester's supervisor reviews the request, and if it is determined that it is appropriate for the requester to have UNIX and DCE accounts, forwards the request to the Operations Supervisor (OPS Super). If the requester requires a National Agency Check (NAC) before access is granted, the OPS Super will forward the request to the Security System Engineer who will then ensure that procedures in Section 3.4.1 are followed before the request is sent to the System Administrator (SA). The OPS Super reviews the request and forwards it to the System Administrator (SA). The SA verifies that all required information is contained on the form. If it is, the SA implements the request. (Incomplete forms are returned to the requester's supervisor for additional information.) After the user is registered, the SA provides the user with a password to use for logging onto their accounts. The SA also sends an e-mail message to the user's supervisor and the OPS Super, informing them that the user's accounts were created.

The **Activity Checklist** table that follows provides an overview of the adding a user process.

Table 3.4-1. Adding a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete User Registration Form and forward to the Supervisor.	(I) 3.4.1	
2	Requester	If privileged access is required, complete NASA Form 531 and forward to the Security System Engineer.	??	
3	Security System Engineer (SSE)	Forwards completed NASA Form 531 to the EDF Security Administrator and maintains privacy of the requestor.	??	
4	EDF Security Administrator	Collects completed NASA Form 531 and forwards to the COTR for further processing. Sends approval notices to the SSE.	??	
5	Security System Engineer (SSE)	Adds NAC completion date to the User Registration Form and forwards to the Supervisor.	??	
6	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.1	
7	OPS Super	Review Request and Forward to SA.	(I) 3.4.1	
8	SA	Review User Registration Form for Completeness.	(I) 3.4.1	
9	SA	Add User.	(P) 3.4.1	
10	SA	Phone/e-mail User with Password. Notify Supervisor and OPS Super that user was added. Notifies SSE when privileged accounts are created.	(I) 3.4.1	

Table 3.4-1 Adding a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Complete User Registration Form and forward to the Supervisor.	(I) 3.4.1	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.1	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.1	
4	SA	Review User Registration Form for Completeness.	(I) 3.4.1	
5	SA	Add User.	(P) 3.4.1	
6	SA	Phone/e-mail User with Password. Notify Supervisor and OPS Super that user was added.	(I) 3.4.1	

Depending upon the script utilized, in order to add a new user the SA should obtain information such as the following about the requester:

a. **Real name of the new user**

b. **User name of the new user**

c. **Office number of the new user**

d. **Office phone number of the new user**

e. **Home phone number of the new user**

f. **Organization**

g. **Group affiliation(s)**

h. **Role(s) of the new user**

The SA creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

3.4.3 Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to the user's supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Supervisor reviews the request and forwards it to the SA, who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.

The Activity Checklist table that follows provides an overview of the deleting a user account process.

Table 3.4-2. Deleting a User - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Determine that No Useful Files Remain in the User's Home Directory and Submit Request to user's Supervisor.	(I) 3.4.2	
2	OPS Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.2	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.2	
4	SA	Delete User.	(P) 3.4.2	
5	SA	Notify Requester, Supervisor and OPS Super that user was deleted.	(I) 3.4.2	

The process assumes that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

a. **UNIX login of the user to be deleted**

a. **Role(s) of the user to be deleted**

The SA deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion, deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

3.4.4 Changing a User Account Configuration

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Supervisor detailing what to change about the account configuration and the reason for the change. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The OPS Supervisor or the Security System Engineer reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

The Activity Checklist table that follows provides an overview of the changing a user account configuration process.

Table 3.4-3. Change a User Account Configuration - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to OPS Supervisor. For privileged accounts submit Request to SSE.	(I) 3.4.3	
2	OPS Super	Review and Forward to SA.	(I) 3.4.3	
3	SSE	Review and Forward to SA.		
4	SA	Change User Account Configuration.	(P) 3.4.3	
5	SA	Inform Requester and Supervisor of completion.	(I) 3.4.3	

The process assumes that the requester's application for changing a user account configuration has already been approved by the OPS Supervisor. In order to perform the procedure, the SA must have obtained the following information from the requester:

a.€ **What to change and new settings.**

Can be any of:

New Real User Name

New Login ID

New Office Number

New Office Phone Number

New Home Phone Number

New UNIX Group

New Login Shell

b. **Current UNIX Login of the User**

- The SA changes the appropriate configuration items manually in the users home directory.

3.4.5 Changing User Access Privileges

The Changing User Access Privileges process begins when the requester submits a request to the supervisor. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The supervisor or the Security System Engineer approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and OPS Super.

The Activity Checklist table that follows provides an overview of the changing user access privileges process.

Table 3.4-4. Changing User Access Privileges - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.4	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Super.	(I) 3.4.4	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.4	
4	SA	Change User Access Privileges.	(P) 3.4.4	
5	SA	Inform Requester, Supervisor and DAAC Mgr of completion.	(I) 3.4.4	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing user access privileges has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **Role(s) to which the user is to be added**

b. **Role(s) from which the user is to be removed**

c. **UNIX login of the user**

To change user access privileges for the requester, execute the procedure steps that follow:

3.4.6 Changing a User Password

The Changing a User Password process begins when the requester submits a request to the SA. The SA verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

The **Activity Checklist** table that follows provides an overview of the changing a user password process.

Table 3.4-5. Changing a User Password - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to SA.	(I) 3.4.5	
2	SA	Verify that the Requester is Who S/he Claims to Be.	(I) 3.4.5	
3	SA	Change Password.	(P) 3.4.5	
4	SA	Inform Requester of completion.	(I) 3.4.5	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management and that the SA is a Tivoli administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New password for the user**

To change a user password for the requester, execute the procedure steps that follow:

3.4.7 Checking a File/Directory Access Privilege Status

The Checking a File/Directory Access Privilege Status process begins when the requester submits a request to the SA. The SA checks the file/directory access privilege status and reports the status back to the requester.

The **Activity Checklist** Table 3.4-6 that follows provides an overview of the checking a file/directory access privilege status process.

Table 3.4-6. Checking a File/Directory Access Privilege Status - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit a Request to the SA.	(I) 3.4.6	
2	SA	Check a File/Directory Access Privilege Status.	(P) 3.4.6	
3	SA	Inform Requester of completion and Report the File/Directory Access Privilege Status.	(I) 3.4.6	

Detailed procedures for tasks performed by the SA are provided in the sections that follow. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which privilege status is needed**

Table 3.4-12 contains a table which presents the steps required to check a file/directory access privilege status in a condensed manner. If you are already familiar with the procedure, you may prefer to use the quick-step table. If you are new to the system, or have not performed this task recently, you should use the detailed procedure presented below.

To check a file/directory access privilege status for the requester, execute the procedure steps that follow:

1 At a UNIX prompt, type **cd *Path***, press **Return**.

- The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe then type **cd /home** and press **Return**.

2 Type **ls -la | grep *FileOrDirectoryName***, press **Return**.
This command will return information like this:

```
drwxr-xr-x  19 jdoe user      4096 Jun 28 09:51 jdoe
-r-xr--r--   1  jdoe user       80  Jun 22 11:22 junk
```

What this output means, from left to right, is:
The file type and access permissions:
The *first character* indicates what type of file it is:
d means that the file is a directory.
- means that the file is an ordinary file.
l means that the file is a symbolic link.

The *next three characters* indicate the owner privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the owner (jdoe) of the file ***junk*** does not have *write* permissions, so a - appears rather than a w.

The *next three characters* indicate the group privileges, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder. ***Example:*** the group (user) of the

directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the sixth character in the line.

The *next three characters* indicate the privileges that everyone else/other has, in the order: **r** = read **w** = write **x** = execute. **-** is a place holder.
Example: other in the case of the directory ***jdoe*** does not have write permissions, so a - appears rather than a w as the ninth character in the line.

There are 19 links to the file/directory ***jdoe***.
The owner of the file/directory is jdoe.
The file/directory's group is user.
The file/directory is 4096 bytes large.
The last time the file/directory was modified is Jun 28 at 09:51.
The name of the file/directory is jdoe.

3 Create a report of the file/directory's access privilege status by using the information produced by step 2 and by filling out this template:

full path of the file/directory: _____

owner: _____

group: _____

owner/user privileges: _____ **read** _____ **write** _____ **execute**

group privileges: _____ **read** _____ **write** _____ **execute**

everyone else/other privileges: _____ **read** _____ **write** _____ **execute**

To check a file/directory access privilege status, execute the steps provided in the following table.

Table 3.4-7. Check a File/Directory Access Privilege Status - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**cd *Path***	**press Return**
2	**ls -la | grep *FileOrDirectoryName***	**press Return**
3	(No entry)	**generate a file/directory access privilege status report**

3.4.8 Changing a File/Directory Access Privilege

The Changing a File/Directory Access Privilege process begins when the requester submits a request to the supervisor to have file/directory access privileges changed. The supervisor approves/denies the request. When approved, the request is forwarded to the OPS Supervisor who reviews the request and forwards it to the SA. The SA changes the file/directory access privileges and then notifies the requester, supervisor and OPS Supervisor of completion.

The **Activity Checklist** table that follows provides an overview of the changing a file/directory access privilege process.

Table 3.4-8. Changing a File/Directory Access Privilege - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to the Supervisor.	(I) 3.4.7	
2	Super	Approve/Deny Request. If Approve, Forward Request to OPS Supervisor.	(I) 3.4.7	
3	OPS Super	Review Request and Forward to SA.	(I) 3.4.7	
4	SA	Change a File/Directory Access Privilege.	(P) 3.4.7	
5	SA	Inform Requester, Supervisor and OPS Supervisor of completion.	(I) 3.4.7	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a file/directory access privilege has already been approved by the supervisor. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **full path of the file/directory on which access privileges will be changed**

b.€ **new access privileges to set on the file/directory. Can be any of:**

New owner

New group

New user/owner privileges (read, write and/or execute)

New group privileges (read, write and/or execute)

New other privileges (read, write and/or execute)

To change a file/directory access privilege for the requester, execute the procedure steps that follow:

1 At the UNIX prompt, type **su**, press **Return**.

2 At the **Password** prompt, type ***RootPassword***, press **Return**.
- Remember that ***RootPassword*** is case sensitive.
- You are authenticated as root.

3 Type **cd *Path***, press **Return**.
- The ***Path*** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory /home/jdoe then type **cd /home** and press **Return**.

4 If there is a **New owner** then type **chown** ***NewOwner FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type: (You must be /home)
  chown ***NewOwner*** **jdoe** and press **Return**.

5 If there is a **New group** then type **chgrp** ***NewGroup FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chgrp ***NewGroup*** **jdoe** and press **Return**.

6 If there are **New user/owner privileges** then type **chmod u=*NewUserPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chmod u=*NewUserPrivileges* jdoe and press **Return**.

- The ***NewUserPrivileges*** are **r** = read **w** = write **x** = execute. To give the user/owner read, write and execute privileges, type:
  chmod u=rwx ***FileOrDirectoryName*** and press **Return**.

7 If there are **New group privileges** then type **chmod g=*NewGroupPrivileges FileOrDirectoryName***, press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. ***Example:*** if the requester wants access privileges changed on directory /home/jdoe then type: (You must be in /home)
  chmod g=*NewGroupPrivileges* jdoe and press **Return**.

- The ***NewGroupPrivileges*** are **r** = read **w** = write **x** = execute.
  Example: to give the group read and execute privileges, type:
  chmod g=rx ***FileOrDirectoryName*** and press **Return**.

8 If there are **New other privileges** then **type:**
chmod o=*NewOtherPrivileges FileOrDirectoryName*, and press **Return**.

- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe then type:
  chmod o=*NewOtherPrivileges* jdoe, and press **Return**.

- The ***NewOtherPrivileges*** are r for read, w for write and x for execute. For example, to give other read privileges, type:
  chmod o=r *FileOrDirectoryName* and press **Return**.

9 Type **exit**, press **Return**.

- Root is logged out.

To change a file/directory access privilege, execute the steps provided in the following table.

Table 3.4-9 contains a table which presents the steps required change a file/directory access privilege.

Table 3.4-9. Change a File/Directory Access Privilege - Quick-Step Procedures

Step	What to Enter or Select	Action to Take
1	**su**	**press Return**
2	***RootPassword***	**press Return**
3	**cd *Path***	**press Return**
4	**chown *NewOwner FileOrDirectoryName***	**press Return**
5	**chgrp *NewGroup FileOrDirectoryName***	**press Return**
6	**chmod u=*NewUserPrivileges FileOrDirectoryName***	**press Return**
7	**chmod g=*NewGroupPrivileges FileOrDirectoryName***	**press Return**
8	**chmod o=*NewOtherPrivileges FileOrDirectoryName***	**press Return**
9	**exit**	**press Return**

3.4.9 Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the OPS Supervisor. The OPS Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and OPS Supervisor.

The Activity Checklist table that follows provides an overview of moving a user's home directory process.

Table 3.4-10. Moving a User's Home Directory - Activity Checklist

Order	Role	Task	Section	Complete?
1	Requester	Submit Request to OPS Supervisor.	(I) 3.4.8	
2	OPS Super	Approve/Deny Request in Accordance with Policy. Forward to SA if approved.	(I) 3.4.8	
3	SA	Move a User's Home Directory.	(P) 3.4.8	
4	SA	Inform Requester and OPS Super of completion.	(I) 3.4.8	

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for moving a user's home directory has already been approved by DAAC Management and that the SA is an administrator. In order to perform the procedure, the SA must have obtained the following information about the requester:

a. **UNIX login of the user**

b. **New location for home directory**

To move a user's home directory for the requester, execute the procedure steps that follow:

3.5 Security

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. To monitor and control access to network services, ECS Security Services uses the public domain tool, TCP Wrappers. Three other public domain COTS products — Anlpassword, Crack, and SATAN — provide additional password protection for local system and network access. The tool, Tripwire, monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for M&O personnel to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

3.5.1 Generating Security Reports

3.5.1.1 Reviewing User Activity Data

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file **/var/adm/loginlog**. The procedures assume that the file has been created and the operator has logged on as root.

Reviewing User Activity Data Procedure

1 At the UNIX prompt, type **/usr/bin/logins [-admopstux] [-g group..] [-l login..],** then press **Return/Enter**.

2 Type **logins -x -l *username,*** then press **Return/Enter**.

- Displays login status for a user:

3 Type **/var/adm/loginlog**, then press **Return/Enter**. To enable login Logging, this creates the log file **loginlog**.

4 Type **chmod 600 /var/adm/loginlog,** then press **Return/Enter**. This sets read and write permissions for root on the file.

5 Type **chgrep sys /var/adm/loginlog,** then press **Return/Enter**. This sets the group to **sys**.

3.5.1.2 Monitoring and Reviewing User Audit Trail Information

The **audit_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

/etc/security/audit_startup

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the audit_control file and re-initialize the current audit directory to the first directory listed in the audit_control file or to open a new audit file in the current audit directory specified in the audit_control file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

Audit Commands Procedures

1 **audit -n**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

2 **audit -s**, then press **Return/Enter**.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

3 **audit -t**, then press **Return/Enter**.

- Signals audit daemon to close the current audit file, disable audit and die.

4 **praudit -sl *filename***, then press **Return/Enter**.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file /usr/include/sys/audit.h. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.